UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,789	03/26/2004	Yoshihiro Hori	65933-082	7144

20277   7590   12/10/2009
MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER
GERGISO, TECHANE

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
12/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/809,789	HORI ET AL.
	Examiner	Art Unit	
	TECHANE J. GERGISO	2437	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2009*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 12-17* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 12-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *November 02, 2009*.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on November 16, 2009 has been entered.

Information Disclosure Statement

2.   The information disclosure statement (IDS) submitted on November 02, 2009 is in

compliance with the provisions of 37 CFR 1.97.   Accordingly, the information disclosure

statement is being considered by the examiner.

Response to Arguments

3.   Applicant's arguments with respect to claims 1-3 and 12-17 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a whole

would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-3 and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blumenau et al. (hereinafter referred to as Blumenau, US Pat. No.: 6,260, 120) in view of McClannahan (US Pat. No.: 6,438, 670) and further in view of Kitahara et al. (hereinafter referred to as Kitahara, US. Pat. No.: 7,082, 539).

As per claim 1:

Blumenau discloses a host device operative to input data to a removable storage device provided with a first storage encryption unit and output data from the storage device, the host device comprising:

a second encryption unit configured to perform a host-device side of a series of cryptographic processing for encrypting data to be secure; and a controller which divides the series of cryptographic processing into a plurality of procedures (column 38: lines 1-10, lines 53-67 and column 40: lines 20-34; the examiner considered a key generation, encryption, decryption, inputting data to be encrypted, outputting the decrypted data, and any other intermediary steps in the cryptographic processing from start to end are considered as plurality of procedures), and

divides the plurality of procedures to be executed in the first encryption unit and procedures to be executed in the second encryption unit, and issues to the storage device a command for controlling the first encryption unit to execute the procedures to be executed in the first encryption(column 35: lines 5-25; lines 53-67; command line).

Blumenau does not explicitly teach the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device in order to have the next procedures executed by the first encryption unit. McClannahan, in an analogous art, however teaches the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device in order to have the next procedures executed by the first encryption unit (column 3: lines 22-33; column 5: lines 12-25; column 6: lines 5-25; The memory storage device of the type having a predetermined timing parameter that defines a minimum delay between the first and second memory control operations). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Blumenau to include the controller obtains information for estimating time necessary to execute the command from the storage device prior to the issuance of the command, sets a wait time for the command based on the obtained information, issues the command to the storage device, and waits the time set for the command before it issues a command for the next procedure to the storage device in order to have the next procedures executed by the first encryption unit. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have

been motivated to do to provide a more flexible and extensible memory controller design that is capable of supporting a wider variety of memory storage devices as suggested by McClannahan (in column 2: lines 60-66).

Blumenau and McClannahan do not explicitly teach the controller issues a command to the storage device via a bus electrically connecting the host device and the storage device, releases the bus for another command. Kitahara, in an analogous art, however teaches the controller issues a command to the storage device via a bus electrically connecting the host device and the storage device, releases the bus for another command (Figure 16: Disk system controller). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blumenau and McClannahan to include the controller issues a command to the storage device via a bus electrically connecting the host device and the storage device, releases the bus for another command. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do to provide an information processing apparatus in which a semiconductor chip serving as a CPU thereof integrally contains a RAM, a cryptographic processing algorithm memory, a cryptographic processing hardware circuit, a key information generating hardware circuit, and a key information storage hardware circuit as suggested by Kitahara in (column 2: lines 20-249).

As per claim 2:

McClannahan discloses a host device, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command (column 11: lines 11-20; column 5: lines 11-24).

As per claim 3:

McClannahan discloses a host device, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a hash operation, a random number generating operation, and log retrieval which are used to execute the command (column 5: lines 11-24; lines 30-38).

As per claim 12:

Blumenau discloses a method for executing a series of cryptographic processing for encrypting data to be secured and inputting or outputting the data between a removable storage device provided with a first encryption unit and a host device provided with a second encryption unit, comprising:

dividing the cryptographic processing into a plurality of procedures, and dividing the plurality of procedures into procedures to be executed in the first encryption unit and procedures to be executed in the second encryption unit(column 38: lines 1-10, lines 53-67 and column 40: lines 20-34; the examiner considered a key generation, encryption, decryption, inputting data to be encrypted, outputting the decrypted data, and any other intermediary steps in the cryptographic processing from start to end are considered as plurality of procedures); and

allowing the second encryption unit to execute the procedures to be executed in the second encryption unit; allowing the host device to issue a command to the storage device in order to control the first encryption unit to the procedures to be executed in the first encryption unit; allowing the to storage device receive the command; and allowing the first encryption unit to execute the command (column 28; lines 35-50, column 35: lines 5-25; Figure 33: 422-430).

Blumenau does not explicitly the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure to the storage device, in order to have the next procedure executed by the encryption unit. McClannahan, in an analogous art, however teaches the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure to the storage device, in order to have the next procedure executed by the encryption unit (column 3: lines 22-33; column 5: lines 12-25; column 6: lines 5-25). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Blumenau to include the host device obtains information for estimating time necessary for the storage device to execute the command from the storage device prior to the issuance of the command, issues the command to the storage device, and waits the time estimated necessary to execute the command before it issues a command for the next procedure

to the storage device, in order to have the next procedure executed by the encryption unit. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide a more flexible and extensible memory controller design that is capable of supporting a wider variety of memory storage devices as suggested by McClannahan (in column 2: lines 60-66).

Blumenau and McClannahan do not explicitly teach the controller issues a command to the storage device via a bus electrically connecting the host device and the storage device, releases the bus for another command. Kitahara, in an analogous art, however teaches the controller issues a command to the storage device via a bus electrically connecting the host device and the storage device, releases the bus for another command (Figure 16: Disk system controller).. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blumenau and McClannahan to include the controller issues a command to the storage device via a bus electrically connecting the host device and the storage device, releases the bus for another command. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do to provide an information processing apparatus in which a semiconductor chip serving as a CPU thereof integrally contains a RAM, a cryptographic processing algorithm memory, a cryptographic processing hardware circuit, a key information generating hardware circuit, and a key information storage hardware circuit as suggested by Kitahara in (column 2: lines 20-249).

As per claim 13:

Blumenau discloses a method, wherein the cryptographic processing is divided into any of process units, the divided process units including:

receiving data input from the host device and performing encryption or decryption using the cryptographic processing unit if necessary (Figure 32: 565, 366, 79; column 37: lines 56-67; column 38: lines 55-65);

performing encryption, decryption, or signature attachment using the cryptographic processing unit in order to output data to the host device (Figure 32: 565, 366, 79; column 37: lines 56-67; column 38: lines 55-65); and

outputting data to the host device, and the command is issued by each of the process units divided (Figure 32: 565, 366, 79; column 37: lines 56-67; column 38: lines 55-65).

As per claims 14 and 15:

McClannahan discloses a method, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary to execute the command (column 11: lines 11-20; column 5: lines 11-24).

As per claims 16 and 17:

McClannahan discloses a method, wherein the information for estimation includes any one of a typical processing time, an average processing time, and a maximum processing time necessary for at least one basic process out of an encrypting operation, a decrypting operation, a

hash operation, a random number generating operation, and log retrieval which are used to execute the command (column 5: lines 11-24; lines 30-38).

Conclusion

6.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

Contact Information

7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to TECHANE J. GERGISO whose telephone number is (571)272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

        Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Techane J. Gergiso/

Primary Examiner, Art Unit 2437